## REMARKS

Favorable reconsideration of this application, as presently amended and in light of the following discussion, is respectfully requested.

Claims 1-12 are pending, with Claims 1, 2, 7, and 8 amended by the present amendment.

In the Official Action, Claims 1, 2, 4, 7, 8, and 10 were rejected under 35 U.S.C. § 102(e) as being anticipated by Angelo et al. (U.S. Patent No. 6,581,162, hereinafter "Angelo"); and Claims 3, 5, 6, 9, 11, and 12 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Angelo in view of Kisliakov (U.S. Patent Publication No. 2003/0212895).

Claims 1, 2, 7, and 8 are amended to more clearly describe and distinctively claim Applicants' invention. Support for these amendments is found in Applicants' originally filed specification.[1] No new matter is added.

Briefly recapitulating, Claim 1 is directed to a data communication apparatus including:

> a memory space;
>
> a service memory field in the memory space, the service memory field being comprised of one or more user blocks, each of the user blocks storing data for providing a corresponding service;
>
> two or more service defining blocks in the memory space, each of the service defining blocks including a service definition data and an access right data which defines an access right to a corresponding user block; and
>
> a PIN-code service definition block in the memory space for defining a PIN-code service which verifies a PIN code before the service is provided, wherein
>
> the PIN-code service defining block includes a PIN-code service block configured to store PIN-code service data so that the PIN-code or the necessity to input the PIN-code vary

[1] Specification page 17, line 7 through page 18, line 6.

> from one access right to another relative to the corresponding user block, and
>
> the one or more user blocks are accessed by using any of the corresponding two or more service defining blocks.

A characteristic feature of the present invention is that an access right to a service memory field is not a universal access right, but that a PIN-code is set for ***each*** access right for ***each*** service conducted in the service memory field. Alternatively, a restriction may be put into place so that a PIN-code must be input in order to write information in the memory area but the PIN-code is not needed to read information from the memory area.[2] Claim 7 is directed to a corresponding method.

Angelo describes a secure environment for entering and storing information necessary to conduct encryption processes. A user password is entered via a secure keyboard channel. The password is maintained in a secure memory space that is not accessible during normal computer operation. In addition to a user password, optional noted identification information is stored in the secure memory. The noted identification information is appended to the user password, and both are subsequently encrypted by an encryption algorithm and encryption keys are also stored in the secure memory. Following encryption, the encrypted data is communicated directly from the secure memory to network interface circuitry for communication over a network. In another embodiment, data entered in a secure manner is used as an encryption key for securely encrypting packets of data prior to communicating the data over a computer network. The encryption key data entered by the user is securely stored for use in multiple encryption processes during a communication session, thereby alleviating the overhead of repeated key renegotiation that is typically required. In addition, an

[2] Specification page 17, line 7 through page 18, line 6.

encryption key that is no longer needed can be safely destroyed in the secure memory without the danger of identified copies of the key remaining in the computer memory.[3]

In particular, Angelo discloses a safestart routine where a user is prompted to enter encryption key information during start-up. This information is stored in a secure computer memory that is accessible while the computer system is in a system management mode. After the information is entered, a latch is set to prevent unauthorized modification of the initial hash values. Thus a secure environment for the creation storage and use of encryption keys is in a distributing computer environment is established.[4]

However, Angelo fails to disclose the multiple PIN-code feature of Applicants' claimed invention. As noted in Applicants' originally filed specification,[5] in order to hierarchically control an access right to each memory field, a PIN-code can be sent to each area, in addition to each application. By inputting a PIN-code corresponding to a certain area, the user can obtain an access right to all applications in the area through verification and authentication processes. In addition the PIN-code can be set for each access right. That is for each service conducted in a service memory field there will be a separate PIN-code. For example, when two services "read" and "read/write", two PIN-codes are set. Likewise, different PIN-codes are set for "addition" and "subtraction" to/from valuable information including electronic money. Alternatively, a restriction may be put into place so that a PIN-code must be input in order to write information in a memory field but a PIN-code need not be input in order to read information from the memory field. The safestart routine of Angelo does not include Applicants' multi-PIN operations.

MPEP § 2131 notes that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art

[3] Angelo, Abstract.
[4] Angelo column 10, lines 20-44.
[5] Specification page 17, line 7 through page 18, line 6.

reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). See also MPEP § 2131.02. "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Because Angelo does not disclose or suggest all the features recited in Claims 1 and 7, Angelo does not anticipate the invention recited in Claims 1 and 7, and all claims depending therefrom.

Kisliakov describes a method and apparatus for executing messages using a plurality of applications resident in a memory means of an electronic card. The electronic card is adapted for coupling to a reader device to facilitate reading of the memory means. The reading device is configured to communicate with a remote apparatus having a further application executing thereon. One or more card resident applications are required to process one or more messages received from the further application. Depending on the determination, the one or more messages are executed using a first of the card resident applications if one or more predetermined criteria are met. Alternatively, the one or more messages are executed using a second of the card resident applications if certain criteria are met. The one or more further criteria are determined via an array containing the one or more criteria.[6] However, Kisliakov does not cure the deficiencies of Angelo.

[6] Kisliakov, Abstract.

Accordingly, in view of the present amendment and in light of the previous discussion, Applicants respectfully submit that the present application is in condition for allowance and respectfully request an early and favorable action to that effect.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Michael Monaco

Bradley T. Lytle
Attorney of Record
Registration No. 40,073

Michael E. Monaco
Registration No. 52,041

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 03/06)
MM/rac

BDL:MEM\dt
I:\ATTY\MM\250822US-AM.DOC